# CYBERSECURITY:
# IMPEGNI, SFIDE E OPPORTUNITÀ PER LE IMPRESE

**Avv. Enrico Di Fiorino LL.M.**
Partner

Fornari e Associati
Milano - Roma - Bari

FORNARI E ASSOCIATI
STUDIO LEGALE

# Normativa

La Direttiva (UE) n. 2022/2555, nota come “**Direttiva NIS2**”, del Parlamento europeo e del Consiglio, del 14 dicembre 2022, relativa a misure per un livello comune elevato di cybersicurezza nell'Unione europea, è la legislazione dell'UE in materia di *cybersicurezza*.

Aggiorna le norme dell'UE in materia di *cybersicurezza* introdotte nel 2016, modernizzando e uniformando il quadro giuridico esistente. Fa parte di un pacchetto di strumenti giuridici e di iniziative a livello sovranazionale, mirato ad aumentare la resilienza di soggetti pubblici e privati alle minacce nell'ambito cibernetico.

Con il decreto legislativo 4 settembre 2024, n. 138, l’Italia ha recepito nell’ordinamento nazionale la Direttiva NIS2, abrogando la precedente direttiva (e il d.lgs. 65/2018).

## Stakeholders

Il decreto conferma il ruolo dell'**ACN** come Autorità nazionale competente NIS e Punto di contatto unico. Sono inoltre identificati **9 Ministeri** quali autorità di settore, che supportano l'attuazione della normativa con la propria competenza settoriale, collaborando nel contesto del Tavolo per l'attuazione della disciplina NIS presieduto da ACN, a cui prendono parte anche rappresentanti della Conferenza permanente per i rapporti tra lo Stato, le Regioni e le Province autonome di Trento e di Bolzano.

## Destinatari

La nuova normativa NIS amplia il campo di applicazione della normativa a **18 settori** di cui 11 altamente critici (originariamente erano 8) e 7 critici (di nuova introduzione) per oltre **80 tipologie di soggetti**, distinguendo i soggetti tra **essenziali** e **importanti**.

L'identificazione è automatica sulla base di **criteri oggettivi** (da media imprese in su). La normativa riguarda oggi l'**intera infrastruttura ICT** del soggetto (originariamente solo reti e sistemi serventi i servizi essenziali).

Fonte: *https://www.acn.gov.it/portale/nis/ambito*

| Settore | Dettaglio | Grandi imprese | Medie imprese | Piccole e micro imprese |
|---|---|---|---|---|
| **SETTORI ALTAMENTE CRITICI** | | | | |
| Energia | 19 tipologie di soggetto | Essenziali | Importanti * | Fuori ambito ** |
| Trasporti | 10 tipologie di soggetto | | | |
| Settore bancario | DORA Lex specialis | | | |
| Infrastrutture dei mercati finanziari | | | | |
| Settore sanitario | 5 tipologie di soggetto | | | |
| Acqua potabile | 1 tipologia di soggetto | | | |
| Acque reflue | 1 tipologia di soggetto | | | |
| Infrastrutture digitali | 9 tipologie di soggetto | | | |
| Gestione dei servizi TIC (b2b) | 2 tipologie di soggetto | | Importanti * | Fuori ambito ** |
| Spazio | 1 tipologia di soggetto | | | |
| **SETTORI CRITICI** | | | | |
| Servizi postali e di corriere | 1 tipologia di soggetto | Importanti * | | Fuori ambito ** |
| Gestione dei rifiuti | 1 tipologia di soggetto | | | |
| Fabbricazione, produzione e distribuzione di sostanze chimiche | 1 tipologia di soggetto | | | |
| Produzione, trasformazione e distribuzione di alimenti | 1 tipologia di soggetto | | | |
| Fabbricazione | 6 tipologie di soggetto | | | |
| Fornitori di servizi digitali | 4 tipologie di soggetto | | | |
| Ricerca | 2 tipologie di soggetto | Importanti * | | Fuori ambito ** |
| **ULTERIORI TIPOLOGIE DI SOGGETTI** | | | | |
| Pubblica Amministrazione centrale | 4 categorie di PA | Essenziali | | |
| Pubblica Amministrazione regionale e locale | 11 categorie di PA | Importanti * | | |
| Ulteriori tipologie di soggetti | 4 tipologie di soggetti | Identificazione dell'Autorità | | |

# Fasi

Recepimento:

- 1 ottobre 2024: pubblicazione in Gazzetta Ufficiale del d.lgs.
- 16 ottobre 2024: entrata in vigore

Prima fase (metà ottobre 24 – metà aprile 25):

- Avvio formale di tutti i tavoli settoriali
- Entro febbraio 2025: censimento e registrazione dei soggetti
- Entro marzo 2025: adozione dell'elenco dei soggetti NIS
- Entro aprile 2025: notifica ai soggetti NIS
- Entro aprile 2025: elaborazione e adozione obblighi di base

# Fasi

Seconda fase (metà aprile 25 – metà aprile 26):

- Monitoraggio e supporto
- A partire da gennaio 2026: obbligo di notifica di base
- Entro aprile 2026: elaborazione e adozione del modello di categorizzazione delle attività e dei servizi
- Entro aprile 2026: elaborazione e adozione degli obblighi a lungo termine
- Entro settembre 2026: completa implementazione delle misure di sicurezza di base

Terza fase (da metà aprile 26):

- Categorizzazione delle attività e dei servizi
- Implementazione degli obblighi a lungo termine

## Iter di registrazione

Dal 1° dicembre 2024 al 28 febbraio 2025 i soggetti pubblici e privati a cui si applica la NIS2 devono manifestarsi all'Autorità nazionale competente NIS **registrandosi** sulla piattaforma digitale.

Resta ferma la possibilità per l'Autorità nazionale competente NIS, su proposta delle Autorità di settore, di individuare ulteriori soggetti ritenuti critici. Tali soggetti riceveranno una specifica comunicazione diretta, a valle della quale potranno procedere con la registrazione.

Tale adempimento è necessario per permettere ad ACN di censire i soggetti operanti nei settori vigilati, anche al fine di fornire loro supporto in fase di implementazione degli obblighi, attraverso le articolate attività di monitoraggio e ausilio nel loro percorso condiviso di crescita, disciplinate dall'articolo 35.

La mancata registrazione è punita con una **sanzione amministrativa pecuniaria** con un importo fino al 0.1 % del fatturato annuo su scala mondiale del soggetto.

## Iter di registrazione

La registrazione è prevista dall'articolo 7 del decreto NIS (con modalità, termini e procedimenti definiti dalla Determinazione 38565/2024.

Prima di avviare la registrazione, il soggetto deve designare il punto di contatto, di cui all'articolo 7, comma 1, lettera c) del decreto NIS. In linea generale, il punto di contatto deve essere un dipendente delegato dal rappresentante legale del soggetto.

La registrazione è composta da **tre fasi**: (i) il censimento del punto di contatto, (ii) la associazione al soggetto e (iii) la compilazione della dichiarazione NIS.

Dal primo dicembre si può avviare la registrazione tramite il Portale dei servizi.

Al termine della fase di registrazione, l'Agenzia e le Autorità di settore vaglieranno le dichiarazioni per costituire l'elenco dei soggetti NIS entro fine marzo 2025. Nel mese di aprile 2025, l'Autorità nazionale competente NIS notificherà al domicilio digitale di tutti i soggetti registrati se rientrano effettivamente nell'elenco.

# Obblighi

Per consentire un adeguamento agli obblighi normativi, il decreto introduce il **principio della graduale implementazione degli stessi**. Prevede, infatti, che i primi obblighi di base, per le notifiche di incidente e le misure di sicurezza, vengano definiti a valle delle consultazioni nell'ambito dei tavoli settoriali.

Per favorirne una corretta attuazione, il decreto legislativo stabilisce una differenziata finestra temporale di implementazione: 9 mesi per le notifiche e 18 mesi per le misure di sicurezza, decorrenti dalla data di consolidamento dell'elenco dei soggetti NIS.

Nell'impianto regolatorio è di fondamentale importanza anche il **principio di proporzionalità**, realizzato tramite l'attività di categorizzazione delle attività e dei servizi dei soggetti NIS. L'attività, che dovrà essere condotta a partire dal 2026, consentirà ai soggetti NIS di distinguere, all'interno della loro organizzazione e con il supporto di ACN, i diversi livelli di esposizione al rischio dei propri sistemi informativi e di rete.

A tali sistemi si applicheranno, in confromità con la loro esposizione al rischio, maggiori obblighi finalizzati a innalzarne progressivamente i livelli di sicurezza informatica.

# Obblighi

Si prevede un rafforzamento degli obblighi con:

- l'obbligo di implementare misure di sicurezza in relazione ad almeno 10 ambiti, con un approccio multi-rischio e proporzionale rispetto al rischio posto al sistema informativo e di rete;
- un processo di notifica degli incidenti più articolato;
- un rafforzamento dei poteri di esecuzione, ispettivi e sanzionatori; le sanzioni si allineano a quanto già previsto dal GDPR in materia *privacy*.

Si prevede l'introduzione di nuovi strumenti, quali:

- la divulgazione coordinata delle vulnerabilità (CVD);
- la gestione delle crisi, specie a carattere transfrontaliero, con l'istituzione del *Cyber crisis liaison organisation network* (CyCLONe) e dell'Autorità nazionale competente per la gestione delle crisi informatiche.

# Obblighi

Alcuni obblighi di rilievo:

Registrazione e aggiornamento dati (articolo 7):

I soggetti che si riconoscono in uno dei settori/sottosettori/tipologie previsti dalla nuova normativa NIS2 dovranno registrarsi su una piattaforma messa a disposizione dall'ACN e comunicare una serie di informazioni tra le quali, ad esempio, la ragione sociale, l'indirizzo e i recapiti aggiornati, la designazione di un punto di contatto indicando il suo ruolo/qualifica presso il soggetto. Ove possibile, i soggetti dovranno anche selezionare uno o più settori/sottosettori in cui operano, tra quelli previsti dagli allegati I, II e III, e la relativa tipologia di soggetto in cui si identificano tra quelle previste dagli allegati I, II, III e IV.

I dati raccolti saranno impiegati per costituire l'elenco dei soggetti NIS, entro il 31 marzo 2025.

# Obblighi

Organi di amministrazione e direttivi (articolo 23):

Sono individuate precise responsabilità in capo agli organi di amministrazione del soggetto, i quali approvano e sovraintendono all'implementazione delle misure oltre a essere responsabili delle eventuali violazioni.

Obblighi in materia di misure di sicurezza informatica (articolo 24):

I soggetti essenziali e i soggetti importanti adottano misure tecniche, operative e organizzative adeguate e proporzionate alla gestione dei rischi posti alla sicurezza dei sistemi informativi e di rete che tali soggetti utilizzano nelle loro attività o nella fornitura dei loro servizi, nonché per prevenire o ridurre al minimo l'impatto degli incidenti.

# Obblighi

Tali misure sono basate su un **approccio multi-rischio**, volto a proteggere i sistemi informativi e di rete nonché il loro ambiente fisico da incidenti, e comprendono almeno i seguenti elementi:

- politiche di analisi dei rischi e di sicurezza dei sistemi informativi e di rete;
- gestione degli incidenti, ivi incluse le procedure e gli strumenti per eseguire le notifiche;
- continuità operativa, ivi inclusa la gestione di backup, il ripristino in caso di disastro, ove possibile, e la gestione delle crisi;
- sicurezza della catena di approvvigionamento, ivi compresi gli aspetti relativi alla sicurezza riguardanti i rapporti tra ciascun soggetto e i suoi diretti fornitori o fornitori di servizi;
- sicurezza dell'acquisizione, dello sviluppo e della manutenzione dei sistemi informativi e di rete, ivi comprese la gestione e la divulgazione delle vulnerabilità;
- politiche e procedure per valutare l'efficacia delle misure di gestione dei rischi per la sicurezza informatica;
- pratiche di igiene di base e di formazione in materia di sicurezza informatica;
- politiche e procedure relative all'uso della crittografia e, ove opportuno, della cifratura;
- sicurezza e affidabilità del personale, politiche di controllo dell'accesso e gestione dei beni e degli assetti;
- uso di soluzioni di autenticazione a più fattori o di autenticazione continua, di comunicazioni vocali, video e testuali protette, e di sistemi di comunicazione di emergenza protetti da parte del soggetto al proprio interno, ove opportuno.

# Obblighi

Obblighi in materia di notifica di incidente (articolo 25):

I soggetti essenziali e i soggetti importanti devono **notificare**, **senza ingiustificato ritardo**, al **CSIRT (Computer Security Incident Response Team) Italia ogni incidente che ha un impatto significativo sulla fornitura dei loro servizi**.

Ai fini della notifica, i soggetti interessati trasmettono al CSIRT Italia:

- senza ingiustificato ritardo, e comunque entro 24 ore da quando sono venuti a conoscenza dell'incidente significativo, una pre-notifica che, ove possibile, indichi se l'incidente significativo possa ritenersi il risultato di atti illegittimi o malevoli oppure possa avere un impatto transfrontaliero;
- senza ingiustificato ritardo, e comunque entro 72 ore (24 ore nel caso di un prestatore di servizi fiduciari) da quando sono venuti a conoscenza dell'incidente significativo, una notifica dell'incidente che, ove possibile, aggiorni le informazioni già trasmesse nella pre-notifica e indichi una valutazione iniziale dell'incidente significativo, comprensiva della sua gravità e del suo impatto, nonché, ove disponibili, gli indicatori di compromissione;
- una relazione finale entro un mese dalla trasmissione della notifica di incidente.

# Obblighi

Banca dei dati di registrazione di nomi di dominio (articolo 29):

I gestori di registri dei nomi di dominio di primo livello e i fornitori di servizi di registrazione dei nomi di dominio raccolgono e mantengono dati di registrazione dei nomi di dominio accurati e completi in un'apposita banca dati con la dovuta diligenza, conformemente al diritto dell'Unione europea in materia di protezione dei dati personali.